UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, v. ASHRAF OMAR ELDARIR, Defendant.	**MEMORANDUM AND ORDER** 20-CR-243 (LDH)

LASHANN DEARCY HALL, United States District Judge:

On January 22, 2020, Ashraf Omar Eldarir ("Defendant") was arrested at John F. Kennedy International Airport ("JFK") on suspicion of illegally transporting Egyptian artifacts. Prior to his arrest, Defendant was subjected to a border search by U.S. Customs and Border Patrol ("CBP"), which included a warrantless search of Defendant's iPhone. Defendant was later charged with two counts of smuggling, in violation of 18 U.S.C. § 545. (Indictment, ECF No. 9.) Defendant now moves to suppress the evidence seized from his iPhone, and any fruits of that evidence, on Fourth and Fifth Amendment grounds. (Def.'s Mem. Law Supp. Mot. Suppress ("Def.'s Mot. Suppress"), ECF. No. 35.)

BACKGROUND[1]

In January 2020, the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), began investigating Defendant after "receiving information that [Defendant] ha[d] been selling Egyptian antiques of suspicious provenance from as early as 2013." (Aff. Supp. Warrant ¶ 14, ECF No. 35-3.) Defendant, a United States citizen and resident of Brooklyn, travels to Egypt frequently through JFK. (*Id.* ¶ 15.) On or about January

[1] The facts are taken from the Defendant's motion to suppress ("Def.'s Mot. Suppress," ECF No. 35), accompanying exhibits (ECF Nos. 35-1, 35-2 and 35-3), Defendant's supplemental brief in support of his motion to suppress ("Def.'s Suppl. Mem.," ECF No. 58) and the November 3, 2021 evidentiary hearing transcript. (*See* Nov. 3, 2021 Evidentiary Hearing Transcript ("Tr.").)

22, 2020, while Defendant was returning to the United States from an international trip to Egypt, CBP agents stopped Defendant at JFK at the direction of HSI. (*Id.* ¶ 16.) Defendant was traveling with one carry-on bag and three checked suitcases that he claimed at the baggage carousel. (*Id.*)

Agents directed him to a secondary customs screening area, where Defendant provided a written declaration stating that he was bringing goods valued at $300 into the country and, when asked, denied transporting artifacts into the United States. (*Id.*) At the secondary customs screening area, CBP agents examined Defendant's luggage and found "bubble and foam wrapped articles in all three checked suitcases." (*Id.*) "Loose sand or dirt came out of the suitcases as they were opened and as the items were unwrapped," with CPB agents noting that some of the items "smelled of wet earth." (*Id.*) The agents found a total of 590 alleged artifacts in Defendant's suitcases. (*Id.*) The agents also found several documents listing previous sales of artifacts with Defendant's name on them, as well as provenances—documents that purport to provide a chronology of an item's ownership—that Defendant claimed were created by his grandfather dating back to the 1920s. (*Id.* ¶ 18.) The provenances were "written in Arabic on watermarked paper with stamps affixed on the top right of the documents, and two-hole punches along the left-hand side." (*Id.*)

CBP agents also found in Defendant's luggage blank paper resembling that of the purported provenances, with the same watermark and two-hole punches along the left-hand side. (*Id.*) Thirteen loose stamps similar to the ones used on the provenances were also found. (*Id.*) According to the Government, the Arabic on some of the provenances found in Defendant's luggage was more modern and not in use during the time the provenances were allegedly written. (*Id.* ¶ 19.) The Government further contends that some of the stamps on the provenances appear

to have been lifted off another document for reuse. (*Id.*) When asked if he had ever sold historical artifacts, Defendant stated "in sum and substance" that he had sold a few in the last few years. (*Id.* ¶ 17.)

CBP agents pulled artifacts out of Defendant's bags at the secondary customs screening area for about an hour. (Evid. Hearing Tr. 19:6–22, 107:6–8.) Then, agents walked Defendant to a separate, pat-down examination room. (*Id.* 19:6–22.) In the pat-down room, one of the agents picked up Defendant's cell phone, which was on a table, and asked Defendant for his passcode. (Def.'s Suppl. Mem. at 4, ECF No. 58; *see also* Tr. 110:11–18.) Defendant was subsequently Mirandized. (Def.'s Suppl. Mem. at 4.)

The agents then "manually searched" Defendant's phone, meaning they opened the device and viewed its contents as any regular user would. (Search and Seizure Warrant ("Warrant"), ¶ 20, ECF No. 35-2; *see also* Def.'s Mot. Suppress at 3.) The agents found additional evidence of artifact smuggling during this manual search in a WhatsApp album that contained photos of artifacts on the ground at night. (Warrant ¶ 20.) Defendant left the airport the same day. (Def.'s Suppl. Mem. at 4.) The Government forensically imaged Defendant's phone on January 23, 2020, which is akin to making a digital copy of the phone to freeze its contents. (Tr. 183:11–17.) The Government subsequently secured a warrant a couple of weeks later, on February 6, 2020, to conduct a forensic search of the phone. (*See generally* Warrant.) No forensic review of the phone was conducted prior to the warrant, meaning the Government did not review the forensic image at that time. (*Id.* 159:24–160:4.)

And, though the Government had Defendant's passcode, HSI agents would have been able to conduct a forensic search of the phone without it. (*Id.* 193:8–14.) Moreover, HSI Special Agent Igor Gamza, who obtained the warrant, testified that he would have sought a warrant

independent of the evidence found during the manual search. (Tr. 160:17–24.) That is, based on the nearly 600 artifacts found in Defendant's belongings and the allegedly false statements he made during an interview with agents, Agent Igor would have sought the same warrant. (*Id.*) At the time, Agent Igor had been a special agent for four years and had experience investigating numerous cases of smuggling. (Warrant ¶ 2.) Based on his experience and training, the "use of WhatsApp to share and store photos is consistent with how artifacts looters communicate[.]" (*Id.* ¶ 20.)

DISCUSSION[2]

I. Fifth Amendment Claims

A. Defendant Was Subjected to a Custodial Interrogation

The Fifth Amendment of the Constitution prohibits the government from compelling any individual to be a witness against himself in a criminal case. U.S. Const. Amend. V. "Historically, [this] privilege was intended to prevent the use of legal compulsion to extract from the accused a sworn communication of facts which would incriminate him." *Doe v. U.S.*, 487 U.S. 201, 212 (1988). As such, it is well-established that a prosecutor "may not use statements, whether exculpatory or inculpatory, stemming from custodial interrogation of [a] defendant unless it demonstrates the use of procedural safeguards effective to secure the privilege against self-incrimination." *Miranda v. Arizona*, 384 U.S. 436, 444 (1966). With that said, not all statements made in custody implicate a defendant's Fifth Amendment interests. Rather, the statement must also be "testimonial, incriminating, and compelled." *See Hiibel v. Sixth Jud. Dist. Ct. of Nevada, Humboldt Cnty.*, 542 U.S. 177, 189 (2004).

[2] During the November 3, 2021 argument on Defendant's motion to suppress, the Government agreed to voluntarily suppress eleven photos that were retrieved from Defendant's phone at the airport that neither party can conclusively determine were resident to Defendant's phone (as opposed to being hosted on the cloud) when they were retrieved. (Tr. 16:1–11.)

Defendant argues that CBP officials infringed his Fifth Amendment privilege against self-incrimination when, without providing a *Miranda* warning, they directed him to furnish his own biometric information (i.e., a fingerprint) to gain access to the contents of his cell phone. (Def.'s Mot. Suppress at 4.) As Defendant sees it, "the requirement that [he] unlock and decrypt his cell phone was compulsive, testimonial, and self-incriminating." (*Id*.) The Government, meanwhile, maintains that the Court need not even reach this question because, as a threshold matter, Defendant was never in custody for Fifth Amendment purposes. (*See* Gov't's Mem. Law. Opp'n to Def.'s Mot. Suppress ("Gov't Opp'n.") at 7, ECF No. 36.) On this point, the Court disagrees.

As the Supreme Court has explained, "custodial interrogation . . . mean[s] questioning initiated by law enforcement officers after a person has been taken into custody or otherwise deprived of his freedom of action in any significant way." *Miranda*, 386 U.S. at 444. A formal arrest is not required; rather, "an accused is in 'custody' when, in the absence of an actual arrest, law enforcement officials act or speak in a manner that conveys the message that they would not permit the accused to leave." *United States v. Ali*, 68 F.3d 1468, 1472 (2d Cir. 1995) (quoting *Campaneria v. Reid*, 891 F.2d 1014, 1021 n.1 (2d Cir. 1989)). And, although courts have long recognized a "border exception" to the Fourth Amendment's restrictions on searches and seizures, *see Tabba v. Chertoff*, 509 F.3d 89, 97–98 (2d Cir. 2007), notably, "Supreme Court precedents establish no similar exception to *Miranda's* prophylactic requirement under the Fifth Amendment." *U.S. v. FNU LNU*, 653 F.3d 144, 149 (2d Cir. 2011).

Importantly, "the initial determination of custody depends on the objective circumstances of the interrogation, not on the subjective views harbored by either the interrogating officers or the person being questioned." *Stansbury v. California*, 511 U.S. 318, 323 (1994). In other

words, the test for determining a suspect's custodial status is "whether a reasonable person in the defendant's position would have understood himself to be subjected to the restraints comparable to those associated with a formal arrest." *Ali*, 68 F.3d at 1472 (internal quotations omitted). As outlined by the Second Circuit in *United States v. FNU LNU*, 653 F.3d 144 (2d Cir. 2011), this inquiry considers a number of factors, in view of the totality of the circumstances:

> "Imagining oneself in 'the suspect's position' necessarily involves considering the circumstances surrounding the encounter with authorities. Those circumstances include, inter alia, the interrogation's duration; it's location (e.g., at the suspect's home, in public, in a police station, or at the border); whether the suspect volunteered for the interview; whether the officers used restraints; whether weapons were present and especially whether they were drawn; whether officers told the suspect he was free to leave or under suspicion . . . and especially so in border situations, the nature of the questions asked."

Id. at 153.

The Government insists that Defendant was neither in custody nor subject to interrogation because his interactions with law enforcement at the border amounted to nothing more than a routine border inspection. (Gov't Opp'n at 6–8.) Relying on *FNU LNU*, the Government notes that "a reasonable traveler arriving at an American airport, like JFK, will expect some constraints as well as questions and follow-up about his or her citizenship, authorization to enter the country, destination, baggage[,] and so on." (*Id.* (citing *FNU LNU*, 653 F.3d at 153–54)). But, on this record, it is clear to the Court that Defendant's experience at JFK on January 22, 2020 went well beyond the routine "constraints and questions" that a reasonable traveler would expect to encounter during a standard border inspection.

Indeed, the cases upon which the Government relies illustrates this point. In *United States v. Carr*, 63 F. Supp. 3d 226 (E.D.N.Y. 2014), for example, the defendant was selected for a CBP examination at JFK Airport, during which officers began to suspect him

of transporting illegal narcotics. *Id*. at 230. Thereafter, he was "physically removed from the public screening area and escorted by four armed officers to a separate, private pat-down room." *Id*. at 236. No guns were drawn, and the defendant was not immediately placed under arrest upon being taken to the pat-down room. *Id*. Nevertheless, the court held that "the totality of the circumstances, including [defendant's] removal from the public area to the private pat-down room, the manner in which he was escorted by two officers, each with both hands on [defendant], and the CBP-dominated atmosphere in the room, strongly suggest a degree of restraint associated with formal arrest." *Id*. So too here.

The Government acknowledges that Defendant was "stopp[ed] him at secondary" and held there for "about an hour," while CBP went through his luggage. (Tr. 19:4–7.) Thereafter, Defendant was "approached by two agents and Officer Hernandez," taken into a pat-down room, subjected to a pat-down search, and asked to unlock his cell phone.[3] (*Id*. 19:11–14; 110:11–18.) Officer Hernandez conceded on cross-examination that Defendant was not free to leave during this process. (*Id*. 132:13–18.) Moreover, at some point while confined to the pat-down room, Defendant asked to use the restroom, and was escorted there by Officer Hernandez, who remained posted outside the door in the event that Defendant tried to "escape." (*Id*. 140:17–141:7.) Subsequently, Agents Gamza and Fromkin entered the pat-down room, read Defendant a *Miranda* warning, and proceeded to interview him for about an hour. (*Id*. 21:5–13.) After the interview was terminated, Defendant remained at the airport for a "couple hours" longer while CBP continued to

[3] The pat-down room is a "secure room" located within a "secure area" of the airport terminal, through a set of "double doors which . . . no other passengers could go through[.]" (Tr. 90:5–10.) During a pat-down search, the passenger is required to remove any outer layers of clothing and empty his pockets, after which officers "pat down [the passenger's] bod[y] to make sure there's nothing extra concealed on [his] person." (*Id*. 90:1–3.) Importantly, not all passengers selected for secondary screening are subjected to a pat-down search. (*Id.* 90:16–18.)

process the items found in his luggage. (*Id*. 21:14–18.) Under these circumstances, the Court cannot conclude that a reasonable person would have felt free to voluntarily terminate the interaction with CBP and HSI personnel and leave. Accordingly, the Court finds that Defendant was in custody during his secondary screening on January 22, 2020.

B. Defendant's Act of Unlocking His iPhone Was Not Testimonial

Even so, the Government cannot be said to have infringed Defendant's privilege against self-incrimination if it did not induce Defendant to make a testimonial communication—that is, one which conveys an "express or implied assertion of fact or belief." *Pennsylvania v. Muniz*, 496 U.S. 582, 597 (1990) ("Whenever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity, or silence, and hence the response . . . contains a testimonial component.") Notably, testimonial communications are not required to be oral or written statements; acts that imply assertions of fact may also fall within the ambit of the Fifth Amendment. *Doe*, 487 U.S. at 208–210. For example, the Supreme Court has recognized that "the act of production could constitute protected testimonial communication because it might entail implicit statements of fact: by producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic." *Id*. at 209 (collecting cases).

But, whether the use of biometric features to unlock a phone can give rise to a testimonial communication is a novel question, one which the Second Circuit has yet to address and which has divided courts elsewhere. *Compare United States v. Wright*, 431 F. Supp. 3d 1175, 1187–88 (D. Nev. 2020), *aff'd*, No. 20-10303, 2022 WL 67341 (9th Cir. Jan. 6, 2022) (finding that defendant's Fifth Amendment rights were violated "because the unlocking of [defendant's] phone with [his] face was a testimonial act") *with Matter of*

Search Warrant Application for cellular telephone in U.S. v. Barrera, 415 F. Supp. 3d 832, 842 (N.D. Ill. 2019) ("[T]o equate the concept of witness, which was originally conceived to cover compelled and incriminating oral testimony, with a fingerprint press is inconsistent with the plain text of the Fifth Amendment"); *see also Matter of Search of [Redacted] Washington, D.C.*, 317 F. Supp. 3d 523, 534, 540 (D.D.C. 2018) (concluding that the use of defendant's biometric information to unlock his phone was "obviously compulsive and was likely to be incriminating," but not testimonial). Importantly, "if a *compelled* act is not *testimonial*, and therefore not protected by the Fifth Amendment, it cannot become protected simply because it will lead to *incriminating* evidence." *Barrera*, 415 F. Supp. 3d. at 836 (emphasis in original) (citing *Doe*, 487 U.S. at 208 n. 6). The critical inquiry is whether, in compelling Defendant to unlock his phone, the Government required Defendant to "disclose the contents of his own mind." *Doe*, 487 U.S. at 210–211 (quoting *Curcio v. United States*, 354 U.S. 118, 128 (1957)) (noting that the government may, among other things, compel a blood sample, a handwriting exemplar, a voice exemplar, and the defendant's participation in a lineup without implicating the Fifth Amendment because "the suspect was not required to 'disclose any knowledge he might have,' or 'to speak to his guilt.'") (citation omitted).

The Court is mindful that "[m]odern cell phones are not just another technological convenience," and that "[w]ith all they contain and all they may reveal, they hold for many Americans the 'privacies of life.'" *Riley v. California*, 573 U.S. 373, 403 (2014). Nevertheless, the Court is persuaded by the weight of authority in other circuits, which holds that the compelled use of a defendant's biometric features to unlock a phone does not amount to a testimonial communication, and therefore does not run afoul of the Fifth Amendment. *See*

Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 794 (D. Idaho 2019) (determining, "in accordance with a majority of [c]ourts that have weighed in on this issue," that compelling defendant's use of a fingerprint to unlock his phone "would not violate the Fifth Amendment because it does not require the suspect to provide any testimonial evidence.").

Particularly persuasive on this point is the Northern District of Illinois' analysis in *Matter of Search Warrant Application for cellular telephone in United States v. Barrera*, 415 F. Supp. 3d 832 (N.D. Ill. 2019). There, the Government applied for a warrant to search the defendant's iPhone for evidence of threats against a confidential informant. *Id.* at 834. In connection with that effort, the Government also sought to compel the defendant to "place his fingers and thumbs on the iPhone home button in an attempt to unlock the phone." *Id.* Before issuing the warrant, the court analyzed whether it was empowered to authorize such a request under the Fifth Amendment. *Id*. at 835. Applying the comparison set forth in *Doe v. United States*, which recognized that "the Fifth Amendment permits the government to force an individual to surrender a key to a strongbox containing incriminating documents, but not to reveal the combination to a subject's wall safe," the *Barrera* court concluded that, "in the context of an iPhone, a finger is a modern substitute for a key," and thus did not undermine the defendant's Fifth Amendment interests. *Id*. at 839 (citing *Doe*, 487 U.S. at 210 n. 9).

Defendant argues that the compelled use of a biometric feature to unlock a phone is testimonial, because it "implicitly conveys testimonial facts about an individual's control over that device and the data it contains, effectively authenticating evidence to be used against him in a way that 'far exceeds the "physical evidence" created when a suspect submits to fingerprinting.'" (Def.'s Mot. Suppress at 8.) And, as Defendant notes, some courts have agreed

with him on this point. A magistrate judge in the Northern District of California, for example, denied a warrant application where the Government sought to compel the use of biometric features to unlock a phone, because "the act concede[d] that the phone was in the possession and control of the suspect, and authenticate[d] ownership or access to the phone and all of its digital contents." *Matter of Residence in Oakland, California*, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019). And, in *United States v. Wright*, a court in the District of Nevada came to the same conclusion, reasoning:

> First, a biometric feature is functionally the same as a passcode, and because telling a law enforcement officer your passcode would be testimonial, so too must the compelled use of your biometric feature to unlock a device. Second, unlocking a phone with your face equates to testimony that you have unlocked the phone before, and thus you have some level of control over the phone.

431 F. Supp. 3d at 1187 (internal citations omitted). The argument is not altogether unpersuasive. The argument, however, seems to disregard the illustration drawn by analogy by the Supreme Court in *Doe*, 487 U.S. at 210 n. 9. That is, in *Doe*, the Supreme Court determined that "[w]e do not disagree with the dissent that '[t]he expression of the contents of an individual's mind' is testimonial communication for purposes of the Fifth Amendment. We simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind. In our view, such compulsion is more like 'be[ing] forced to surrender a key to a strongbox containing incriminating documents' than it is like 'be[ing] compelled to reveal the combination to [petitioner's] wall safe.'" *Id.* (citation omitted). By extension, a fingerprint, like a key:

> "[R]equires no revelation of mental thoughts. Nor does a finger require a communication of any information held by that person[.] In fact, the application of a finger to the home button on a iPhone 'can be done while the individual sleeps or is unconscious,' and thus does not require any revelation of information stored in a person's mind."

Barrera, 415 F. Supp. 3d at 839 (quoting *Google Pixel 3 XL Cellphone*, 398 F. Supp. 3d at 794).

Moreover, the compelled use of a fingerprint to unlock an iPhone does not, as Defendant suggests, necessarily imply ownership or control of it. For example, an iPhone with "Touch ID" capabilities, such as the iPhone 7 in the instant case, can store the fingerprints of up to five different individuals.[4] Were the Government to compel any one of those individuals to unlock the phone biometrically, their ability to do so would ultimately say nothing about who actually owned the phone, or was responsible for its contents.[5]

For these reasons, the Court cannot conclude that the compelled use of biometrics to unlock a phone is a testimonial act, thereby implicating the Fifth Amendment. Accordingly, suppression is not warranted on Fifth Amendment grounds.

II. Defendant's Fourth Amendment Claims

A. The Independent Source Doctrine

The Fourth Amendment provides that:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

U.S. Const. Amend. IV. "As the text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness." *Riley*, 573 U.S. at 381–82 (2014) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006) (internal quotations omitted)). The Supreme Court has held that "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, . . . reasonableness generally requires the obtaining of a judicial warrant."

---

[4] *See, e.g.*, *Adding More Fingerprints to iPhone Sensors*, THE NEW YORK TIMES (May 10, 2016), https://www.nytimes.com/2016/05/11/technology/personaltech/adding-more-fingerprints-to-iphone-sensors html; *see also* Glenn Fleishman, *How to add other people's fingerprints to Touch ID*, MACWORLD, (Mar. 17, 2019) https://www.macworld.com/article/232548/how-to-add-other-peoples-fingerprints-to-touch-id html.

[5] Certainly, the compelled disclosure of Defendant's passcode may have constituted a testimonial act. Defendant concedes, however, that he initially unlocked his iPhone at the request of CBP officers using his fingerprint. (Def.'s Aff. ¶ 3, ECF No. 35-1.)

Vernonia School Dist. 47J v. Acton, 515 U.S. 646, 653 (1995). Typically, to remedy a Fourth Amendment violation, i.e., a warrantless search, courts apply the exclusionary rule to exclude unlawfully seized evidence and any fruits thereof. *See, e.g.*, *Segura v. United States*, 468 U.S. 796, 804 (1984) ("[T]he exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and found to be derivative of an illegality or 'fruit of the poisonous tree.'"); *see also Mapp v. Ohio*, 367 U.S. 643, 655 (1961) ("[T]he Fourth Amendment include[s] the exclusion of the evidence seized in violation of its provisions."). But, "the significant costs of this rule have led [courts] to deem it 'applicable only . . . where its deterrence benefits outweigh its substantial social costs.'" *Utah v. Strieff*, 579 U.S. 232, 237 (2016) (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)). Courts have thus recognized several exceptions to the exclusionary rule, one being pursuant to the independent source doctrine. *Id.* at 238.

The independent source doctrine "permits the admission of evidence seized [during] an unlawful search if that evidence would have been obtained through separate, lawful means." *United States v. Vilar*, 729 F.3d 62, 83 n.19 (2d Cir. 2013) (citing *Murray v. United States*, 487 U.S. 533, 537 (1988)). When such evidence is obtained pursuant to a warrant issued after an illegal search, the independent source doctrine applies if, "(1) the warrant [was] supported by probable cause derived from sources independent of the illegal [search]; and (2) the decision to seek the warrant [was] not . . . prompted by information gleaned from the illegal conduct." *United States v. Johnson*, 994 F.2d 980, 987 (2d Cir. 1993). Thus, even assuming the search of Defendant's phone was unconstitutional, suppression is not warranted if (1) the February 6 warrant is supported by probable cause from sources independent of the search of the phone, and if (2) the decision to seek the warrant was not prompted by any of the same information.

And, with respect to the first inquiry, "probable cause is a fluid concept-turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." *Illinois v. Gates*, 462 U.S. 213, 232 (1983). A magistrate's determination of whether probable cause exists requires "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before [it], . . .there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Gates*, 462 U.S. at 238). Moreover, the nexus between the thing to be searched and the alleged criminal activity "may be based on reasonable inference from the facts presented based on common sense and experience." *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004) (internal quotation marks and citation omitted).

Here, the independent source doctrine applies. Subsequent to the manual search and image of Defendant's phone, the Government sought and obtained a warrant to search the device. Agent Gamza's affidavit in support of the warrant set forth the following facts in support of a finding of probable cause, which are not tied to any evidence found on Defendant's phone prior to obtaining the warrant. *See United States v. Reilly*, 76 F.3d 1271, 1282 n.2 (2d Cir. 1996), *on reh'g*, 91 F.3d 331 (2d Cir. 1996) (finding that in determining whether the first prong of the independent source doctrine is satisfied, "a reviewing court should excise the tainted evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant") (citation and alterations omitted):

- HSI began investigating Defendant in January 2020 for artifacts he had allegedly been selling as far back as 2013. (Warrant ¶ 14.)
- Defendant travels to Egypt frequently. (*Id.* ¶ 15.)
- On January 22, 2020, CBP agents uncovered 590 pieces of artifacts in Defendant's luggage when he was returning to the United States from Egypt. (*Id.*

¶ 16.) The articles found smelled of wet earth, and loose sand or dirt came out of Defendant's suitcases when they were opened. (*Id.*)

- When asked if he had ever sold historical artifacts, Defendant stated that he had sold a few within the last few years. (*Id.* ¶ 17.)

- CBP agents uncovered several documents purporting to be provenances as well as 13 loose stamps similar to those affixed to the purported provenances. (*Id.* ¶ 18.)

- According to individuals familiar with Egyptian Arabic, the writing on the provenances was not in use during the time from which they purport to be. (*Id.* ¶ 19.) Similarly, based on information from individuals familiar with Egyptian artifacts, some of the stamps on the purported provenances appear to have been lifted off another document for the purpose of reusing. (*Id.*)

- Based on Agent Gamza's training and experience, the use of WhatsApp to share and store photos is consistent with "how artifacts looters communicate[.]" (*Id.* ¶ 20.)

Moreover, Agent Gamza attested that "[b]ased on [his] knowledge, training and experience, [he] know[s] that electronic devices can store information for long periods of time." (*Id.* ¶ 24.) And, it is undisputed that Defendant was in possession of the phone at the airport when he was accused of illegally importing Egyptian artifacts. (*See, e.g.*, *id.* ¶ 20.) These facts together with those set forth in Agent Gamza's affidavit support a finding of probable cause to search Defendant's phone. *See, e.g.*, *United States v. Hoey*, No. 15-CR-229, 2016 WL 270871, at *9 (S.D.N.Y. Jan. 21, 2016) ("Courts have commonly [ ] found probable cause to search cellphones possessed by defendants arrested in connection with ongoing drug-distribution crimes based on the experience of agents familiar with narcotics trafficking that traffickers commonly use cellphones to communicate in the course of their narcotics distribution, as well as to store relevant information[.]"); *United States v. Robinson*, No. 16-CR-545 (S-3), 2018 WL 5928120, at *16 (E.D.N.Y. Nov. 13, 2018) ("[T]he fact that SCPD discovered the phone at the scene of the crime creates a sufficient factual nexus to justify the search.").

For example, in *United States v. Barret*, 824 F. Supp. 2d 419, 448 (E.D.N.Y. 2011), a special agent included in her warrant affidavit a description of the circumstances leading up to the defendant's arrest. The affidavit described large boxes of drugs found in plain view during the arrest, and attested that, in her experience, cell phones are "capable of electronically storing numerous types of information" and that "individuals involved in narcotics trafficking typically use cellular phones to communicate and store information and other records on their phones." *Id.* Based on those attestations, the court found that there was "ample support" for a probable cause finding to search a defendant's phone for evidence. *Id.* at 449. The same is true here.

The warrant sets forth descriptions of the articles found in Defendant's possession at the airport in January 2020 and information from those familiar with Egyptian artifacts and language that suggest that Defendant was engaged in the illegal importation of artifacts. (*See* Warrant, ¶¶ 14–21.) Moreover, Agent Gamza attests, based on his experience, that phones are capable of storing information for long periods of time and that those engaged in illegal smuggling often use WhatsApp on their phones to communicate. (*Id.* ¶¶ 23–24.) The affidavit also establishes that the phone was in Defendant's possession during the alleged illegal importation and that Defendant had been under investigation leading up to his January 22, 2020 flight to JFK. (*Id.* ¶¶ 14, 20.) The affidavit thus sets forth a sufficient basis for probable cause to search Defendant's phone, even without considering the information gleaned prior to the Government obtaining a warrant.

Notably, Defendant does not challenge the veracity of the statements in Agent Gamza's affidavit. Rather, Defendant takes issue with paragraph 20 of Agent Gamza's affidavit and contends that the entirety of that paragraph must be "excised" from the Court's assessment of

probable cause because the paragraph comes from information learned from Defendant's phone. (Def.'s Reply at 14–17.)

> The relevant substance of paragraph 20 reads:
>
> > CBP agents seized [Defendant's] cell phone (the Device) and manually searched its contents pursuant to the border search doctrine. The border search of the Device revealed evidence of smuggling by [Defendant.] For example, the Device contains photos of stamps like the ones affixed to the purported provenances. Individuals familiar with Egyptian artifacts and provenances have stated that many provenances originating from Egypt in the 1940s had stamps on them so as to add to their authenticity. The Device also contains a WhatsApp album that contains numerous photos of artifacts on the ground at night. Based on my training and experience, the use of WhatsApp to share and store photos is consistent with how artifacts looters communicate, and the location of the items on the ground at night is indicative of looting. . . ."

(*See* Warrant, ¶ 20.) Specifically, Defendant argues that Agent Gamza's "knowledge of [Defendant's] WhatsApp application and his inclusion of information about his training and experience related to WhatsApp" should be excised because, according to Defendant, "[t]here is no reason to believe that the WhatsApp information would have been included in the absence of the agent's knowledge that the WhatsApp application was downloaded on [Defendant's] phone." (Def.'s Reply at 15–16.) Yet, even if the Court were to constructively excise any mention of WhatsApp from the warrant application, Agent Gamza testified persuasively that he would have sought the same warrant based on the nearly 600 artifacts found in Defendant's belongings and the allegedly false statements he made to agents, irrespective of the information found on Defendant's phone. (Tr. 160:17–24.) And, the Court found Agent Gamza to be credible during the November 3, 2021 hearing and credits his testimony. *See, e.g.*, *United States v. Josephberg*, 562 F.3d 478, 487 (2d Cir. 2009) (citations omitted) ("The assessment of witness credibility lies solely within the province of the [fact finder].").

Defendant made no effort to rebut Agent Gamza's testimony on this point and offers nothing to the contrary for the Court's consideration. Indeed, in his supplemental brief following the November 3, 2021 hearing, Defendant does not discuss the independent source doctrine once. The Court finds that Agent Gamza would have obtained a warrant to search Defendant's phone even without the information gleaned from the initial manual search.

Defendant further contends that the Government would not have sought a warrant if they had not compelled Defendant to provide his passcode. (Def.'s Suppl. Mem. at 19–20.) But, Scott Delaney, a certified forensic agent with the Department of Homeland Security, testified that he could have performed an extraction of Defendant's phone for the forensic review even without a passcode, though it may have taken additional time. (Tr. 193:8–14.) The Court found Agent Delaney to be credible and credits this testimony. Notably, Defendant did not cross-examine Mr. Delaney on this point or make any effort to rebut his testimony during the hearing. Instead, in his post-hearing submission, Defendant cites to a number of cases where agents were cross-examined on the programs they used and their personal experience breaking into cell phones to argue that the Government would not have been able to access Defendant's phone in this case. (Def.'s Suppl. Mem. at 19–20 (citing *e.g.*, *United States v. Djibo*, 151 F. Supp. 3d 297, 300 (E.D.N.Y. 2015)). But, Agent Delaney's unequivocal and unrebutted testimony was that he would have been able to access Defendant's phone even without a passcode. Accordingly, the Court finds with high confidence that the evidence Defendant seeks to suppress would have been discovered even if, as Defendant argues, he had not been compelled to unlock the phone. Accordingly, suppression is not warranted on this ground either. *See, e.g.*, *United States v. Jackson*, No. 19-CR-6026, 2020 WL 810747, at *12 (W.D.N.Y. Feb. 19, 2020) ("On this record, I find that the evidence which Jackson seeks to suppress would have been discovered even if

Jackson had not been compelled to provide the passcode to the phone or present his biometric features to unlock the phone"); *United States v. Will*, No. 15-CR-6, 2015 WL 3822599, *16 (N.D. W.Va. June 19, 2015) (finding that suppression not warranted under doctrine of inevitable discovery where evidence demonstrated contents of phone would have been extracted without [a] password); *United States v. Todd*, No. 416-CR-305, 2017 WL 1197849, *13 (S.D. Ga. Feb. 10, 2017) ("as [the agent] testified, [the] FBI offices . . . had the technological capabilities to bypass the swipe pattern and access the contents of [d]efendant's cell phone[;] [t]hus, regardless of whether officers violated [d]efendant's Miranda rights in obtaining [d]efendant's swipe pattern, the inevitable discovery doctrine prevents suppression of the evidence attained from the cell phone search"), *report and recommendation adopted*, 2017 WL 1172113 (S.D. Ga. March 29, 2017).

CONCLUSION

For the foregoing reasons, Defendant's motion to suppress is DENIED.

SO ORDERED.

Dated: Brooklyn, New York
July 6, 2023

/s/ LDH
LASHANN DEARCY HALL
United States District Judge